MINNESOTA GOVERNMENT DATA PRACTICES ACT

INTRODUCTION

The Minnesota Government Data Practices Act is contained in Minnesota Statutes, Chapter 13.The Act regulates the collection, creation, storage, maintenance, dissemination, and access to government data in government entities, including the City of Minneapolis. The Act establishes a presumption that government data are public and are accessible by the public for both inspection and copying unless there is a federal law, a state statute or a temporary classification of data that provides that certain data are not public.

Government data re defined as "... all data collected, created, received, maintained or disseminated by any government entity regardless of its physical form, storage media or conditions of use." Minn. Stat. §13.02, subd. 7. The Act defines three essential data classifications. Data may be public, private, or confidential.

Public data means data which is accessible to the public. Private data on individuals (or non-public data not on individuals) means data which is made by statute or federal law applicable to the data: (a) not public; and (b) accessible to the individual subject of that data. Confidential data on individuals (or protected non-public data not on individuals) means data which is made not public by statute or federal law applicable to the data and is inaccessible to the individual subject of that data.

ACCESS TO GOVERNMENT DATA

As already noted, the Act presumes that all government data are public unless the law dictates otherwise. Public data must be made available for inspection at no charge immediately, if possible, or as soon as possible. If a request is made for copies of public data, the City may require the requesting person to pay the actual costs of searching for and retrieving government data, including the cost of employee time, and for making, certifying, compiling, and electronically transmitting the copies of the data or the data, but may not charge for separating public from not public data. However, if one hundred or fewer pages of black and white, letter or legal size paper copies are requested, actual costs shall not be used. Instead, the City may charge up to twenty-five cents per page. If the City is not able to provide copies at the time a request is made, copies shall be supplied as soon as reasonably possible.

When a request is made by an individual who is the subject of data, the person must be informed as to whether or not they are the subject of stored data and the data's classification. The City must comply with a request for access or copying made by the subject of the data immediately, if possible, or within ten working days of the request if immediate compliance is not possible.

When private or confidential data is collected from an individual, the individual has the right to be informed (a) as to the purpose and intended use for collection of the data, (b) whether the individual may refuse to provide the data, (c) any known consequences of refusing to provide the data and, (d) the identity of persons or agencies authorized to receive the data. Generally speaking, private or confidential data is available only to individuals within the City whose work assignments reasonably require access.

Private or confidential data can only be used in accordance with the advisory given to the individual at the time of the collection of the data. It can only be released pursuant to a court order or with the informed consent of the subject of the data. Informed consent should generally be in writing.

Although the Act presumes that all government data are public, the exceptions tend to overwhelm this presumption. The Act, as it is currently constituted, comprises 115 pages of statutes, most of the pages are dedicated to creating exceptions to the general rule. A few of the most commonly encountered privacy and confidentiality issues are noted below.

Personnel Data

One of the most commonly raised issues involves the classification of personnel data regarding City employees. Personnel data is defined in Minn. Stat. §13.43 as data on individuals collected because the individual is or was an employee of, or an applicant for employment by, performs services on a voluntary basis for, or acts as an independent contractor with the City. The personnel data section of the statute stands alone in that it reverses the ordinary presumption of data classification under the Act. That is, personnel data is deemed private data unless specifically enumerated within the section as public data. The public personnel data is as follows:

(1) Name; employee identification number, which must not be the employee's social security number; actual gross salary; salary range; contract fees; actual gross pension; the value and nature of employer paid fringe benefits; and the basis for and the amount of any added remuneration, including expense reimbursement, in addition to salary;

(2) Job title and bargaining unit; job description; education and training background; and previous work experience;

(3) Date of first and last employment;

(4) The existence and status of any complaints or charges against the employee, regardless of whether the complaint or charge resulted in a disciplinary action;

(5) The final disposition of any disciplinary action together with the specific reasons for the action and data documenting the basis of the action, excluding data that would identify confidential sources who are employees of the public body;

(6) The terms of any agreement settling any dispute arising out of an employment relationship, including a buyout agreement as defined in Minnesota Statutes, Section 123B.143, subdivision 2, paragraph (a); except that the agreement must include specific reasons for the agreement if it involves the payment of more than $10,000 of public money;

(7) Work location; a work telephone number; badge number; and honors and awards received; and

(8) Payroll time sheets or other comparable data that are only used to account for employee's work time for payroll purposes, except to the extent that release of time sheet data would reveal the employee's reasons for the use of sick or other medical leave or other not public data.

(9) All other personnel data are private. The dissemination of personnel data is rife with complications and is often the subject of claims of breach of privacy. The Mayor's Office and Council Members are advised to contact the City Attorney's Office before disseminating personnel data.

Elected Officials' Data

In Minneapolis, full-time elected officials are treated as employees for the purposes of the Data Practices Act. However, financial disclosure statements of elected or appointed officials which, by requirement of the political subdivision, are filed with the political subdivision, are public data. Correspondence between individuals and elected officials is private data on individuals, but may be made public by either the sender or the recipient.

Pending Civil Legal Actions

The Mayor's Office and Council Members should be aware that data collected as part of an active investigation undertaken for the purpose of the commencement or defense of a pending civil legal action, as determined by the City Attorney, is confidential. The data remain confidential until the conclusion of the civil legal action.

Law Enforcement Data

Another category of data of which the Mayor's Office and Council Members should also be aware is comprehensive law enforcement data. Law enforcement data is data created or maintained by agencies carrying on a law enforcement function, including but not limited to the Police and Fire Departments. The Act provides that criminal investigative data is confidential while the investigation is active. The law enforcement data section of the Act also provides for protection of the identities of certain victims and witnesses.

Other Data

Other examples of private data include medical data, certain educational data, certain welfare data, and social security numbers. The Mayor's Office and Council Members should take care to protect the statutory privacy interest of individuals. The City Attorney's Office is always available for consultation on these issues.

REMEDIES FOR VIOLATIONS OF THE ACT

The Data Practices Act provides that a willful violation of its provisions is a misdemeanor. The Act also authorizes a private legal action to enjoin violations of the Act and provides for exemplary damages of not less than $1000, nor more than $15,000 for each willful violation of the Act. If the court issues an order to compel compliance, it may impose a civil penalty of up to $1000 against the government entity. The Act also allows a party prevailing in a suit for damages arising from a violation of the Act to recover costs and disbursements, including reasonable attorneys fees.